AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Derek Dunn, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, being duly sworn, do depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, and have been so employed since April 2003. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to child exploitation and child pornography. I have received training in the area of child pornography and child exploitation, and as part of my duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

2. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request an arrest warrant.

3. I make this affidavit in support of an application for a criminal complaint charging Timothy RYAN with possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). As will be shown below, there is probable cause to believe that RYAN has committed the offense of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

4. This affidavit is based in part on information that I learned from discussions with other law enforcement officers and on my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing an arrest warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that RYAN has committed violations of Title 18, United States Code, Section 2252A(a)(5)(B).

SPECIFIED FEDERAL OFFENSES

5. Title 18, United States Code, Section 2252 prohibits a person from knowingly possessing or accessing with the intent to view sexually explicit images of a minor as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of a minor engaging in sexually explicit conduct.

DEFINITIONS

6. The following definitions apply to this affidavit and Attachment B:

a.) "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

b.) "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

c.) "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons

of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

d.) "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

e.) "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

f.) "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers).

g.) "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h.) "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i.) The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j.) "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

k.) "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

l.) The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON PEER-TO-PEER ("P2P") SOFTWARE

7. Peer-to-peer ("P2P") file-sharing is a method of communication available to Internet users through the use of special software such as BitTorrent. Computers linked together

through the Internet using this software form a network that allows for the sharing of digital files between users on the network. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the information is first deposited before it is distributed. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from one folder to another to stop the distribution across the Internet. Further, once a file or files are placed in a shared folder its distribution is dependent only on the machine being turned on and connected to the Internet.

8. BitTorrent is one type of P2P file-sharing protocol. Users of the BitTorrent network wishing to share new content will use a BitTorrent client to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

9. One of the advantages of P2P file-sharing is that multiple files may be downloaded at the same time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading a movie file may actually receive parts of the movie from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. It is possible to also download the file or files from only one computer.

10. The BitTorrent Network bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the digital fingerprinting of data. Once you check a file or files with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

PROBABLE CAUSE

11. This investigation focuses on an individual sharing child sexual abuse material ("CSAM") on the BitTorrent Network from an IP address associated with the Steele Hill Resort, located at 516 Steele Hill Road in Sanbornton, New Hampshire. The software used by law enforcement uses SHA1 hash values to identify files being shared on the network that have been previously determined to contain child pornography and/or related material. When the software recognizes the SHA1 hash value of such files on the network, it automatically tries to download them. Further, the BitTorrent software used by law enforcement uses a single-source download protocol. In other words, when the software identifies a BitTorrent user that has suspected files

of child pornography available for download, it will initiate a download of the entire file from that single user, as opposed to downloading portions of the target file from multiple users.

12. In 2020, Deputy Frederick James of the Grafton County Sheriff's Department observed that the IP address 64.223.67.220 was a top offender in New Hampshire for supplying CSAM through the P2P network BitTorrent. In fact, observations made from various BitTorrent indices, which provide publicly available information and are used as matchmakers to connect users on the BitTorrent network, revealed that this IP address had consistently been used to distribute CSAM on the BitTorrent network since May 2015.

13. Deputy James observed that Taunton (MA) Police Detective Randy Demello had obtained downloads on April 3, 2020, from the IP address 64.233.67.220 and contacted him to obtain the downloads. Deputy James reviewed Detective Demello's downloads and observed that several of the files were CSAM. In response to a Summons, Consolidated Communications identified that the subscriber for IP address 64.233.67.220 at the time of the download was Steele Hill Resort at 516 Steele Hill Road, Sanbornton, NH. The investigation revealed the address 516 Steel Hill Road is the Administrative Business Office for the resort. The resort is a destination family resort in Sanbornton, NH that specializes in year-round weddings and time share retreats. The resort is surrounded by woods, overlooks the lakes and mountains of New Hampshire, has a nine-hole golf course, indoor and outdoor pools, hiking trails, tennis courts and conference venues.

14. Between 2020 and 2022, Deputy James and other investigators continued to occasionally review the BitTorrent software and continued to observe downloads from the IP address 64.223.67.220. Deputy James conducted research on the resort but could not establish a suspect due to the large number of employees and guests who would likely have access to the

internet at the resort. Given the duration of the P2P activity resolving to the resort as well as the times of day and night that the activity was observed, investigators surmised that the suspect was almost certainly an employee of the resort and likely someone who resided on the property.

15. In June 2022, HSI Task Force Officer Adam Rayho began furthering the investigation. TFO Rayho and Nashua (NH) Police Detective Peter LaRoche maintained an undercover ("UC") BitTorrent software at the Nashua Police Department. As mentioned above, the software focuses on users sharing child sexual abuse material on the BitTorrent Network. Upon reviewing downloads obtained for the months of April, May, and June 2022, TFO Rayho observed fifteen from the IP address 64.223.67.220 on different dates and times. On each of these occasions, the UC software recognized and downloaded files of investigative interest containing CSAM from the IP address. TFO Rayho reviewed each connection to include the files which had been downloaded, and observed the majority contained CSAM and others contained child erotica. A selection of three successful downloads and the related files are outlined in the following paragraphs.

16. On April 29, 2022 at 02:40:24 UTC, the UC BitTorrent software identified a torrent of investigative interest that was available for download from the IP address 64.223.67.220. The SHA1 info hash associated with the torrent was one that had been previously determined to contain CSAM. The UC BitTorrent software connected with the target IP address and successfully downloaded fourteen complete files. One of the downloaded files is described as:

Filename:	45f0a0c9afcde99d6addbe21991a83a8 - 10yo anal bondage cumshot girl man pthc vaginal.avi
Description:	two minute and one second video of a prepubescent female lying on her back with her legs tied at the ankles. An adult male is continually inserting his penis into the prepubescent females vaginal and anal openings while

also occasionally inserting his finger into her vaginal opening. At the conclusion of the video, the male ejaculates on the prepubescent female's stomach.

17. On May 29, 2022 at approximately 12:17:08 UTC, the UC BitTorrent software identified a torrent of investigative interest that was available for download from the IP address 64.223.67.220. The SHA1 info hash associated with the torrent was one that had been previously determined to contain CSAM. The UC BitTorrent software connected with the target IP address and successfully downloaded twenty-nine complete files. One of the downloaded files is described as:

Filename: 2012_Rosemary_March_2012_BJ_CUM_SDC10676.avi

Description: forty-seven second video of a naked prepubescent female lying on her side. An adult male is inserting his penis into the prepubescent female's mouth and eventually ejaculates on the prepubescent female's chest.

18. On June 02, 2022 at approximately 01:44:28 UTC, the UC BitTorrent software identified a torrent of investigative interest that was available for download from the IP address 64.223.67.220. The SHA1 info hash associated with the torrent was one that had been previously determined to contain CSAM. The UC BitTorrent software connected with the target IP address and successfully downloaded two-hundred and fourteen complete files. One of the downloaded files is described as:

Filename: (pthc buratino lolifuck) alena - girl in bed gets wanked over (cumshot) - new 2012.wmv

Description: seven second video of an adult male masturbating over a naked, sleeping, prepubescent female.

19. In June 2022, TFO Rayho sought updated subscriber information for the IP address 64.233.67.220 for the period April 29, 2022 to June 16, 2022. In response to a summons, Consolidated Communications identified the subscriber for IP address 64.233.67.220

during that timeframe was The Summit Resort, with a service address of 516 Steele Hill Road, Sanbornton, New Hampshire. Consolidated Communications advised the service start date was September 27, 2013 and provided an account number which matched the account for the previous legal process issued by Deputy James in 2020 for the IP address 64.233.67.220.

20. Researching The Summit Resort, TFO Rayho learned it had a physical address in Laconia, New Hampshire and appeared to be associated with Steele Hill Resort based on its website. Contact was later made with representatives of the Steele Hill Resort who advised The Summit Resort is a sister company of Steele Hill Resort and is owned under the same parent company. TFO Rayho subsequently contacted Consolidated Communications who advised the company name for the internet account has changed on occasion but that the physical location/service address of the IP address 64.233.67.220 has remained 516 Steele Hill Road, Sanbornton, New Hampshire, which is the Steele Hill Resort.

21. During the month of July 2022, TFO Rayho continued to monitor the UC BitTorrent software and observed an additional thirteen downloads from the IP address 64.233.67.220. One of the successful downloads and related files is described in the following paragraph.

22. On July 13, 2022 at approximately 14:44:45 UTC, the UC BitTorrent software identified a torrent of investigative interest that was available for download from the IP address 64.223.67.220. The SHA1 info hash associated with the torrent was one that had been previously determined to contain CSAM. The UC BitTorrent software connected with the target IP address and successfully downloaded 2,121 complete files. One of the downloaded files is described as:

Filename: Kait_5Yo_Golden_Shower_On_Dad.wmv

Description: five minute and twenty-three second video involving a naked prepubescent female and adult male. The prepubescent female first performs oral sex on the adult male's penis and stimulates the male's penis with her hands. As the video continues, the prepubescent female sits on the male's lap near his penis while the male masturbates.

23. During August and September of 2022, TFO Rayho continued to monitor the UC BitTorrent software and observed downloads of investigative interest similar to the ones referenced above which contain CSAM from the IP address 64.223.67.220.

24. On September 21, 2022, TFO Rayho, Special Agent Shawn Serra, and I made contact with one of the Steele Hill Resort owners (SHRO) and informed him that an individual(s) had been using the resort's internet and IP address to obtain and distribute CSAM for the past several years going back to May 2015. SHRO advised that he was willing to assist law enforcement in attempting to identify the individual(s) responsible for this activity.[1] Through subsequent communications with SHRO, the resort's legal counsel, and outside contractors who maintain the resort's information technology (IT) network, law enforcement learned that IP address 64.223.67.220 has five subnetworks that are part of the wireless internet infrastructure at the resort, some being password protected and others being open networks available to anyone on the property. Given the size of the resort, numerous wireless access points (WAP) are located throughout the property to help ensure that wireless internet service is widely available throughout the property. Connections to this IP address via any of the five wireless networks must be made from devices physically located on the resort property. In addition, due the remote

[1] This individual was approached by law enforcement after a review of his international travel records, which showed that he was out of the country on the dates of some of the illicit activity occurring at the resort. Based on this information, law enforcement considered this individual an unlikely suspect.

location of the resort, a device would not be able to connect to the resort's wireless network from any of the neighboring properties.

25. Based on the information above, the number of years the activity has consistently been observed, and the varying hours of the day and week when activity has been observed, your Affiant suspects that there is one individual responsible for the majority, if not all, of the activity and that this individual has resided on resort property since at least May 2015. In response to legal process, the resort provided information regarding current employees of the resort who have been employed by the resort and resided on the property since on or before May 2015. According to the resort's response, there are only two current employees who meet those criteria—they are Timothy RYAN and D.O.

26. According to resort records, D.O. was hired by the resort in April 2001 and began residing on the property in or about September 2010. Timothy RYAN began working at the property through a job placement agency and submitted a signed employment application with the resort on April 30, 2015. RYAN worked on the resort property first as an employee of the job placement agency beginning on or about May 17, 2015. RYAN then became an employee of the resort on or about May 27, 2015. It is unclear when RYAN moved onto the resort property, but he signed a housing agreement dated May 28, 2015. The timeline associated with the start of RYAN's employment at the resort correlates closely with the start of the BitTorrent activity resolving to the resort's IP address. Both RYAN and D.O. reside in the "Main Inn Building" on the resort property, with RYAN residing in a private room on the third floor and D.O. residing in a private room on the second floor.

27. In effort to identity the device(s) that were connecting to the resort's wireless network to access and distribute CSAM, representatives of the resort consented to law

enforcement monitoring and capturing network traffic information that is transmitted over the resort's wireless network with assigned IP address 64.223.67.220. The network traffic information that law enforcement was authorized to monitor is information that is accessible to the resort and the resort's IT staff.

28. On November 4, 2022, U.S. Secret Service New England Cyber Fraud Task Force (NECFTF) TFO Sergey Vasilyev, HSI Special Agent Jordan Lawi, and I met with representatives of the Steele Hill Resort. TFO Vasilyev set up equipment to monitor and capture network traffic information during the investigation. Capturing network traffic is done by using a computer program to create packet capture files (PCAP). "Packets" are data travelling through a network. Some of this data—specifically, the Media Access or "MAC"[2] address—identifies the specific devices that are connected to the wireless network at a given time. The network traffic information may also identify the particular wireless access point on the property that a particular device is using to access the wireless network.

29. On multiple occasions in November and December 2022, while remotely monitoring network traffic, TFO Vasilyev observed activity on the resort's wireless network that indicated a user of the network was actively using P2P software.

30. On November 14, 2022, at approximately 0815 hours, TFO Vasilyev observed that a device with the MAC address AE:7C:E3:9A:1E:7D was using the resort's wireless network to transmit via the BitTorrent protocol a torrent file with a SHA-1 info hash known by law enforcement to contain CSAM. The firewall logs showed that the device name associated with this P2P network activity was \"Tim-s-Galaxy-A50\". TFO Vasilyev further identified that

[2] A MAC address is a unique identifier associated with an electronic device capable of connecting to a network.

at the time of this activity, the device was connected to a wireless access point that is located in the "Main Inn Building" where RYAN resides.

31. On December 5, 2022, TFO Vasilyev reviewed network traffic logs that showed that \"Tim-s-Galaxy-A50\" with MAC 70:1f:3c:5d:61:79 was active on BitTorrent at approximately 0640 hours and was connected to a wireless access point in the "Main Inn Building" where RYAN resides. The network logs did not show a torrent info hash.

32. On December 7, 2022 from approximately 21:10 to 22:47 hours, TFO Vasilyev observed that a device with the MAC address 70:1f:3c:5d:61:79 was using the resort's wireless network to transmit via the BitTorrent protocol a torrent file with a SHA-1 info hash known by law enforcement to contain CSAM. The firewall logs showed that the device name associated with this P2P network activity was \"Tim-s-Galaxy-A50\". TFO Vasilyev further identified that during the timeframe associated with this activity, the device connected to several wireless access points on the resort property, including access points located in the "Main Inn Building" where RYAN resides.

33. Based on the observation of two distinct MAC addresses, both with the host/device name \"Tim-s-Galaxy-A50\", being associated with P2P activity on the resort's wireless network, TFO Vasilyev believes its likely that RYAN is using at least two different devices to connect to the resort's wireless network.

34. On December 13, 2022, a federal search warrant was executed on RYAN'S person and his residence, a private room on the third floor of the Main Inn Building at the Steele Hill Resort in Sanbornton, NH. RYAN was encountered while working in a guestroom on the resort property. RYAN was advised that there was a federal search warrant for his person and his room. RYAN was further advised that he was not under arrest and that he was free to leave

at any time. RYAN advised that he understood. Agents asked RYAN if he would be willing to speak with them about the investigation, to which RYAN agreed. RYAN agreed to voluntarily accompany agents to an unmarked police vehicle on the property to be interviewed.

35. Upon arriving at the vehicle, RYAN sat in the front passenger seat. He was not handcuffed nor was his freedom of movement restrained in any way. I sat in the driver seat of the vehicle and another agent sat in the rear passenger seat. RYAN was reminded that he was not under arrest, was not required to speak with agents, and that he was free to leave at any time. He was further advised that he could terminate the interview at any time. RYAN was advised that the interview would be audio recorded, to which RYAN agreed. During the interview, RYAN remained seated in the front passenger seat. At various points during the interview, RYAN opened the vehicle door so that he could smoke cigarettes and exited the vehicle on occasion so that he could get fresh air and stretch his legs.

36. During the interview, RYAN was advised that agents were conducting an investigation related to illicit internet activity occurring on the resort property. Initially, RYAN denied familiarity with P2P software. He claimed to have heard the term "uTorrent" but denied any recent use. Later during the interview, RYAN was confronted with the fact that a Samsung cell phone was located in his room and that the investigation suggested that it was a Samsung cell phone identified as "Tim's Samsung Galaxy A50" that appeared to be responsible for the illicit activity occurring on the premises. Upon being confronted with this information, RYAN acknowledged that he was using BitTorrent on the Samsung cell phone to access and download child pornography on the internet.

37. During the search, the following items were seized: a Motorola cell phone seized from RYAN's person, a Samsung Galaxy A50 cellphone seized from RYAN's bedroom and an

Xbox gaming system seized from RYAN's bedroom. While onsite, HSI Special Agent/Computer Forensics Agent (SA/CFA) Shawn Serra obtained a forensic acquisition of the Samsung Galaxy A50. During the acquisition, SA/CFA Serra opened the Google Photos application and immediately observed a video which automatically began playing. The video file indicated in the top right corner that it was 1 hour, 3 minutes, and 6 seconds in length. SA/CFA Serra did not view the entire video; however, the portion of the video that began playing automatically depicted a pre-pubescent naked male laying on his back while a pre-pubescent naked female performed oral sex on him. Further review of the forensic evidence file revealed hundreds of additional images and at least three videos of apparent CSAM.

CONCLUSION

38. Based on the facts set forth above, there is probable cause to believe and I do believe that RYAN has committed violations of Title 18, United States Code, Section 2252A(a)(5)(B), possession of child pornography. Accordingly, I respectfully request that the Court grant the attached application for a criminal complaint.

/s/ Derek Dunn
Derek Dunn
Special Agent
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. P. 41 and affirmed under oath the contents of this affidavit and application.

Andrea K. Johnstone

Hon. Andrea K. Johnstone
United States Magistrate Judge
Date: December 13, 2022